

12/30/99

jc672 U.S. PTO

01-03-00

A

<b>UTILITY PATENT APPLICATION TRANSMITTAL</b>  <i>Only for new nonprovisional applications under 37 C.F.R. § 1.53(b)</i>	Attorney Docket No. <b>A-6307</b>	
	First Inventor or Application No. <b>DeFreeze</b>	
	Title <b>Mechanism and Apparatus for Encapsulation of Entitlement Authorization in Conditional Access System</b>	
	Express Mail Label No. <b>EL 433548144 US</b>	

<b>APPLICATION ELEMENTS</b> See MPEP chapter 600 concerning utility patent application contents		<b>ADDRESS TO:</b> Box Patent Application Assistant Commissioner for Patents Washington DC 20231																	
1. <input checked="" type="checkbox"/> Fee Transmittal Form (e.g. PTO/SB/17) (Submit an original and duplicate for fee processing)		5. <input type="checkbox"/> Microfiche Computer Program (Appendix)																	
2. <input checked="" type="checkbox"/> Specification [Total Pages <u>28</u> ]		6. <input type="checkbox"/> Nucleotide and/or Amino Acid Sequence Submission (e.g. PTO/SB/17) <ul style="list-style-type: none"> <li>a. <input type="checkbox"/> Computer Readable Copy</li> <li>b. <input type="checkbox"/> Paper Copy (identical to computer copy)</li> <li>c. <input type="checkbox"/> Statement verifying identity of above copies</li> </ul>																	
3. <input checked="" type="checkbox"/> Drawings (35 U.S.C. § 113) [Total Sheets <u>4</u> ]		<b>ACCOMPANYING APPLICATION PARTS</b>																	
4. Oath or Declaration [Total Pages <u>5</u> ] <ul style="list-style-type: none"> <li>a. <input type="checkbox"/> Newly executed (original or copy)</li> <li>b. <input checked="" type="checkbox"/> Copy from a prior application (37 C.F.R. § 1.63(d))          (for continuation/divisional with Box 16 completed)           <ul style="list-style-type: none"> <li>i. <input type="checkbox"/> <b>DELETION OF INVENTORS</b>              Signed statement attached deleting inventor(s)              named in the prior application, see              37 C.F.R. §§ 1.63(d)(2) and 1.33(b)</li> </ul> </li> </ul>		7. <input checked="" type="checkbox"/> True Copy of Original Assignment Papers (cover sheet & document(s))																	
16. <input checked="" type="checkbox"/> If a CONTINUING APPLICATION, check appropriate box, and supply the information below and in a preliminary amendment: <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Continuation <input type="checkbox"/> Divisional <input type="checkbox"/> Continuation-in-part (CIP) of prior application No: <u>09/111,958</u></li> </ul> Prior application information: Examiner: Jack, T.. Group Art Unit: <u>2767</u>		8. <input type="checkbox"/> 37 C.F.R. § 3.73(b) Statement (when there is an assignee) <input type="checkbox"/> Power of Attorney																	
		9. <input type="checkbox"/> English Translation Document (if applicable)																	
		10. <input checked="" type="checkbox"/> Information Disclosure Statement (IDS)/PTO-1449 <input type="checkbox"/> Copies of IDS Citations																	
		11. <input type="checkbox"/> Preliminary Amendment																	
		12. <input checked="" type="checkbox"/> Return Receipt Postcard (MPEP 503) (Should be specifically itemized)																	
		13. <input type="checkbox"/> Small Entity <input type="checkbox"/> Statement filed in prior application, Status still proper and desired																	
		14. <input type="checkbox"/> Certified Copy of Priority Document(s) (if foreign priority is claimed)																	
		15. <input type="checkbox"/> Other.																	
<b>17. CORRESPONDENCE ADDRESS</b>																			
<input checked="" type="checkbox"/> Customer Number or Bar Code or <input type="checkbox"/> Correspondence address below																			
<table border="1"> <tr> <td>Name</td> <td colspan="3"></td> </tr> <tr> <td>Address</td> <td colspan="3"></td> </tr> <tr> <td>City</td> <td>State</td> <td>Zip Code</td> <td></td> </tr> <tr> <td>Country</td> <td>Telephone</td> <td>Fax</td> <td></td> </tr> </table>				Name				Address				City	State	Zip Code		Country	Telephone	Fax	
Name																			
Address																			
City	State	Zip Code																	
Country	Telephone	Fax																	

Name (Print/type)	HUBERT J. BARNHARDT III	Registration No. (Attorney/Agent)	36,739
Signature	<i>Hubert J. Barnhardt III</i>	Date	December 30, 1999

Docket No.: A - 6307

**MECHANISM AND APPARATUS FOR ENCAPSULATION OF  
ENTITLEMENT AUTHORIZATION IN CONDITIONAL ACCESS SYSTEM**

5                   **CROSS-REFERENCE TO RELATED APPLICATIONS**

This application claims priority to U.S. provisional application Serial No. 60/054,578, DeFreese et al., filed August 1, 1997 entitled "Mechanism and Apparatus for Encapsulation of Entitlement in Conditional Access System" (Attorney Docket No. T-2910).

10

**BACKGROUND OF THE INVENTION**

Field of the Invention

The present invention relates to a conditional access system such as a conditional access cable television system. In particular, the invention relates to  
15 identification of packages of bundled services, called entitlement units, and the authorization of reception of an entire entitlement unit.

Description Of Related Art

Known conditional access systems individually authorize each service to be  
20 received. For example, a subscriber of a cable television system may subscribe to a plurality of services (e.g., HBO, Cinemax, ShowTime, etc.).

Known conditional access systems provide services to subscribers in tiers. Tiers are used as a way to provide standard service to some subscribers while providing premium services to other subscribers. Each subscriber is assigned to a  
25 specific tier. For example, consider a service that provides two tiers: a standard service that carries over the air broadcast programs and a premium service that carries the standard service plus HBO, Cinemax and ShowTime. Tier authorization data is transmitted from the system's headend to a home communication terminal for each subscriber where it is stored. In this example, the tier authorization data may be a  
30 single bit set to indicate premium service and cleared to indicate standard service. In

PATENT APPLICATION  
DOCKET NO. A-6307

general, many tiers (e.g., 256) may be provided. The tier authorization data may be a number (e.g., from 0 to 255) that indicates the authorized tier. Each tier corresponds to a specific combination of authorized programs out of a list of available programs (e.g., out of 128 available programs). Alternatively, the tier authorization data may be  
5 a long data word (e.g., 128 bits or 16 bytes of 8 bit each) where each bit in the tier authorization data corresponds to an authorized program. The tier authorization data in this example is merely the long data word with as many bits set as there are authorized programs for the tier, and the identification of the authorized programs is by noticing the bit position that is set.

10 No matter how the tier authorization data is encoded, it is transmitted from the headend to a subscriber's home communication terminal. Each subscriber is authorized for a particular tier. A table that relates the tier authorization data for each subscriber to the correspondingly identified home communication terminal is stored in the headend. For each subscriber, the headend prepares a unique addressed message  
15 containing the tier authorization data corresponding to the subscriber, and the headend transmits the data to the subscriber's home communication terminal. Often the data is encrypted by the headend and decrypted by the home communication terminal.

Programs broadcast from the headend are identified by frequency, channel number, digital data stream number, etc. The home communications terminal  
20 processes a subscriber's request for a particular program by determining a number associated with the requested program and verifying that the terminal is authorized to receive a tier that "contains" the program.

**BRIEF DESCRIPTION OF DRAWINGS**

25 The invention will be described in detail in the following description of preferred embodiments with reference to the following figures wherein:

FIG. 1 is a block diagram of the communication system according to the invention;

FIG. 2 is a block diagram of a terminal according to the invention;

FIG. 3 is a block diagram of a processor of the terminal according to the invention;

FIG. 4 is a format diagram of a packetized data transport stream (a multiplex) as processed by the invention;

5        FIG. 5 is a flow chart of a method of determining whether a service is authorized according to the invention;

FIG. 6 is a flow chart of a method of pre-confirming authorization; and

FIG. 7 is a flow chart of a method of post-confirming authorization.

## 10        **DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS**

In FIG. 1, a conditional access communication system includes headend 2, a plurality of home communication terminals 4, and a link therebetween 6. The headend operator may receive content for transmission from a plurality of service providers 8.

15        In FIG. 2, terminal 10 (e.g., as included in home communications terminal 4) includes processor 20, tunable tuner 12, demodulator 14, and control link 16 to control the frequency of tunable tuner 12. Terminal 10 may also include second tuner 22 and demodulator 24 to receive "out of band" data streams.

In operation, headend operators provide a plurality of services. Usually each  
20    service is carried on a separate 6 MHZ channels. To receive a particular service, processor 20 directs tunable tuner 12 by control link 16 to tune to the frequency of the particular service desired. Demodulator 14 demodulates the tuned signal according to its modulation technique (e.g., PSK, QPSK (Quadrature Phase Shift Keying Modulation), Offset QPSK, etc.). Standards have been developed for carrying  
25    wideband video and audio information for a program (e.g., MPEG-2). However, some systems may carry non-MPEG (Moving Picture Experts Group) compliant signals (e.g., IP packets). When this occurs, terminal 10 may include second tuner 22 and demodulator 24 to recover non-MPEG compliant data. Both data streams are processed in processor 20, or separate but coupled processors may be provided.

PATENT APPLICATION  
DOCKET NO. A-6307

In FIG. 3, a more detailed description of processor 20 is depicted. Processor 20 includes secure microprocessor 30 and individual service decryptors 60. Processor 20 also includes demultiplexer 22 to cull encrypted and/or authenticated entitlement control message 28 from the transport data stream input and to cull encrypted  
5 entitlement management message 52 from the transport data stream input. Demultiplexer 22 also culls clear payload text 68 from the transport data stream which is provided to service demultiplexer 26. The transport data stream (TDS) is also provided at 24 to service demultiplexer 26 and may include video signals, a plurality of audio signals, or utility information. Any or all of these separate information data  
10 streams may be separately encrypted. If these information data streams are separately encrypted they will be decrypted, if authorized, in service decryptor 60 as discussed below.

Secure microprocessor 30 includes secure memory 38 that stores multi-session key (MSK), entitlement unit number and a decoder private key (DPK). Secure  
15 microprocessor 30 also includes decryptor 32, decryptor and/or authenticator 34, conditional access logic 36 and authorized control word decryptors 40. Decryptors 32 and 40, decryptor and/or authenticator 34 and conditional access logic 36 may advantageously be implemented in a general purpose arithmetic/logic section and program memory section (having a program stored therein) of secure microprocessor  
20 30. Secure microprocessor 30 is characterized by memory 38 being unobservable at the input/output terminals of secure microprocessor 30. Thus, any intermediate unencrypted data may be stored in memory 38 (preferably non-volatile) without being observable by pirates. Data transferred into or out of secure microprocessor 30 is preferably protected at the terminals of microprocessor 30 by encryption if the data is  
25 long lived or remains unprotected if the data is so short lived that its observation by a pirate is harmless. For example, multi-session key is preferably stable for a period of hours to a month or so. Thus, it is preferably encrypted. In contrast, control words that are decrypted in secure microprocessor 30 from encrypted entitlement control messages typically change every 2 to 5 seconds so that observation of the control  
30 word by a pirate does not seriously compromise the system's security.

When entitlement control messages are transported in the transport data stream in encrypted form, a pirate is unable to observe the entitlement unit numbers and control words contained in the entitlement control message. However, the entitlement control message may also be transported in authenticated form (e.g., keyed secure hash). In authenticated form, the entitlement control message includes two parts: a clear text part and a hashed part. The entitlement control message is authenticated in authenticator 34 of secure microprocessor 30 (FIG. 3) by hashing the clear text part and comparing it to the hashed part of the entitlement control message. If they agree, then the entitlement control message is authenticated. A pirate may be able to observe the clear text part of the entitlement control message; however, if a pirate were to attempt to insert an additional entitlement unit number into the entitlement control message, the comparison of the hashed part and the results of the local hashing will fail. This reveals a modification of the entitlement control message, and the modified message is ignored.

In operation, demultiplexor 22 culls encrypted entitlement management message 52 from the transport or "out of band" data stream and provides it to decryptor 32. Decoder private key is read from secure memory 38 passed through conditional access logic 36 to decryptor 32 where it is used to decrypt and/or authenticate entitlement management message 52. Decoder private key may be a secret key such as those used in the Data Encryption Standard (DES) algorithm or must be the private component of a public/private key pair such as those used in the RSA algorithm. The entitlement management message includes both authorized entitlement unit number to be stored in secure memory 38 and authorized multi-session key to be stored in secure memory 38. Multi-session key is changed from time to time, preferably monthly or more often. When a subscriber wishes to upgrade service and be authorized to receive additional services (e.g., change from HBO only to HBO and Cinemax), a new entitlement management message will be transmitted to the secure microprocessor so that a new entitlement unit number will be recovered by decryptor 32 and stored in secure memory 38.

Encrypted and/or authenticated entitlement control message 28 is culled from the transport data stream input and provided to decryptor and/or authenticator 34. Multi-session key is read from secure memory 38 and passed through conditional access logic 36 to decryptor and/or authenticator 34 at 46. Decryptor and/or authenticator 34 decrypts and/or authenticates the entitlement control message to reveal encrypted control words for each encrypted component (e.g., video, audio, etc.) of the service being carried on the transport data stream and to reveal a list of all entitlement unit numbers to which the currently received service belongs. For example, a first entitlement unit may include both HBO and Cinemax, whereas a second entitlement unit may include only HBO. The entitlement control message for the HBO service (i.e., HBO data stream) would include both the first and second entitlement unit numbers.

Conditional access logic 36 compares the list of entitlement unit numbers from decryptor and/or authenticator 34 with the authorized entitlement unit number stored in secure memory 38. If there is a match, then the service may be received. Conditional access logic 36 will then pass the control words from the decrypted and/or authenticated entitlement control message to the decryptors 40. Control words for individually encrypted service components (e.g., video, audio, etc.) are passed to decryptor 40. In decryptor 40, the control words will be decrypted using the multi-session key to provide clear text versions of the control words, or "service seeds" 62.

Control words are characterized by frequent changes. Whereas, multi-session key may change as infrequently as once a month, control words may change every two to five seconds. The decrypted control words are provided by decryptor 40 at output terminals of secure microprocessor 30. Even if a pirate were to recover a decrypted control word, the decrypted control word is short lived so as to have substantially no value to the pirate.

Service selection data 56 from the decrypted contents from decryptor and/or authenticator 34 is provided to service demultiplexor 26 via control access logic 36. Selected services 64 are provided by service demultiplexor 26 to service decryptor 60

PATENT APPLICATION  
DOCKET NO. A-6307

at 64 based on service selection 56. Service decryptor 60 processes encrypted services of the selected services 64 using seeds 62 to provide decrypted services 66.

In FIG. 4, a representative transport data stream 70 (called a multiplex) is depicted. The transport data stream is packetized in packets of 188 bytes. Each packet includes a synchronization block and a prefix. Payload data may be concatenated between a plurality of transport packets to form a packetized elementary stream as depicted at the top of FIG. 4. One packetized elementary stream depicted at the bottom of FIG. 4 is the network information table (NIT). The network information table carries such information as a table of direct correspondence between a multiplex number and a frequency (for tuner 12 of FIG. 2) in which the data stream may be found.

Other information may be provided with the network information table. For example, entitlement unit table (EUT) in which each service, identified by universal service identification number (USID) is included together with each entitlement unit number to which the service belongs. Alternatively, the entitlement unit table may be transported "out of band" and received in processor 20 via tuner 22 and demodulator 24 (FIG. 2).

Similarly, in order to aid a user to select a desired service, service information may be provided over a permanently available data link (e.g., a data link not switched with the selected program) as either "in band" or "out of band" data. For example, an out of band data link may be a 108 MHz phase shift keyed (e.g., QPSK) broadcast data link. In band might be specific data packets in the data stream at a predetermined initial tuned frequency. Permanently available in band data link data might also be data packets carried in the data stream of all tunable frequencies. Such service information provides a list of services (i.e., universal service identification numbers) corresponding to each data stream number. Preferably, additional text is carried with the service information for each service so as to enable the terminal to include a electronic program guide.

In FIG. 4, program association table (PAT) is carried as payload data in packet 0 of multiplex 70. The program association table includes a list of each program



available and a corresponding packet number at which program map table (PMT) may be found. There is a program map table for each program. The program map table includes a list of each component of the program (e.g., audio and video, entitlement control messages, etc.) and a packet number at which the program component (e.g.,  
5 audio, video, entitlement control messages, etc.) may be found. Of particular importance is the program component that is the entitlement control message since it specifies all entitlement unit numbers to which the program belongs. The program map table includes information directing where the entitlement control message for that program may be found. This enables demultiplexor 22 (FIG. 3) to cull the  
10 encrypted entitlement control message 28 from the transport data stream.

Also of importance is conditional access table (CAT) found in packet 1 of multiplex 70 (FIG. 4). The conditional access table has for each system type of secure microprocessor (e.g., 30 in FIG. 3) in the system, a packet identification number where the encrypted entitlement management messages may be found. This packet  
15 number enables demultiplexor 22 to cull the encrypted entitlement management message 52 from the transport data stream (FIG. 3). Further filtering based on the address of the secure micro-processor may then be performed.

In FIG. 5, method 100 for determining whether a terminal is authorized to receive a service is practiced in processor 20 (FIG. 2). At step 102 data is read from  
20 the data stream. This data includes the entitlement unit table and the service information. At step 104, a user selects a desired service associated with a universal service identification number (e.g., as may be used with an electronic program guide). This may be accomplished through any of the known electronic program guide techniques. The entitlement unit table from the network information helps translate  
25 the universal service identification number into entitlement unit numbers that belong to the service. At step 110, the secure microprocessor pre-confirms whether the authorized entitlement unit number stored in secure memory 38 (FIG. 3) is a member of the entitlement unit numbers in the entitlement unit table that corresponds to the selected service. If it is not a member, at step 106, a message may be displayed to the  
30 user (e.g., displayed on a television style monitor) and the user will be requested to

select another service. Alternatively, the terminal may automatically step to the next service, or to any predetermined service such as a barker channel.

It will be noted that a service pirate may attempt to add extra entitlement unit numbers to the entitlement unit table. However, based on the present invention, the  
5 pirate will still be unable to recover the service.

When it is determined at step 110 that a service is authorized, at step 124, tuner 12 is directed to tune to the desired service. This information comes from the network information table that associates the universal service identification number with the frequency on which the service may be received. After tuner 12 tunes to the  
10 correct frequency, demodulator 14 recovers the digital data stream carried at the tuned frequency. At step 130 (FIG. 5), the digital data stream is decrypted. At step 150, the decrypted digital data stream is decompressed (e.g., decompression from the compressed MPEG format) and then displayed to the user.

Step 110 (FIG. 5) is further described with reference to FIG. 6. The  
15 entitlement unit table has a list of all entitlement unit numbers that carry the specified service. In a loop that includes steps 112, 114, 116, 118 and 120, all entitlement unit numbers from the entitlement unit table are tested. At step 112, the first (and in later iterations the next) entitlement unit number belonging to the selected service is read from the entitlement unit table. At step 114, the entitlement unit number from the  
20 entitlement unit table is sent to the secure microprocessor to be compared to the authorized entitlement unit number stored in secure memory 38 (FIG. 3). If the comparison is favorable, then the service is declared authorized at step 116, and the tuner tunes to the service (step 124, FIG. 5). If the comparison is unfavorable, then at step 118, a test is made to determine whether all entitlement unit numbers from the  
25 entitlement unit table have been tested. If all entitlement unit numbers from the entitlement unit table have been tested and none has been the authorized entitlement unit number stored in secure memory 38, then the service is declared not authorized. However, if there are still more entitlement unit numbers from the entitlement unit table to be tested, then the next entitlement unit number is read in steps 120 and 112,  
30 and the loop is repeated.

PATENT APPLICATION  
DOCKET NO. A-6307

This pre-tuning testing procedure has human factors benefits. Subscribers who tend to "surf" through the channels will tend to grow impatient if the time required to produce a display exceeds 1 second, and this delay will be relatively unnoted if the time to produce the display is less than 1/4 of a second. It is therefore desirable to provide a quick way to determine whether a service is authorized or unauthorized before tuner 12 is directed to tune to a particular frequency. It should be noted that the entitlement unit table may not be, and is not required for this purpose, to be secure. It may be sent unencrypted.

In FIG. 7, decrypting the service in step 130 is described in more detail. Processor 20 preferably includes a general purpose microprocessor performing step 132. Step 132 includes acquiring program association table and program map table at step 134.

At step 136, the general purpose microprocessor directs demultiplexor 22 to cull the encrypted and/or authenticated entitlement control message 28 (FIG. 3) from multiplex 70 (FIG. 4). The encrypted and/or entitlement control message is then sent to secure microprocessor 30 (FIG. 3) to be decrypted and/or authenticated.

At step 140, the encrypted and/or authenticated entitlement control message is decrypted and/or authenticated in the secure microprocessor, and the authorized entitlement unit number stored in secure memory 38 (FIG. 3) is compared to the list of entitlement unit numbers to which the present desired service belongs as listed in the decrypted and/or authenticated entitlement control message. This confirmation process takes place after tuner 12 tunes to the desired frequency. Since the entitlement control message is encrypted and/or authenticated, a pirate would not be able to insert false entitlement unit numbers into the entitlement control message without be detected.

When it is confirmed that the authorized entitlement unit number (stored in secure memory 38) is the same as one of the entitlement unit numbers carried in the entitlement control message, one or more control words are recovered from the entitlement control message. These control words correspond to each individual component of the service and are provided at 50 to decryptor 40 (FIG. 3). The control

PATENT APPLICATION  
DOCKET NO. A-6307

words are decrypted using multi-session key in decryptor 40 to provide seeds for decryption of service components in service decryptor 60.

In step 138 (FIG. 7), service selection data 56 (FIG. 3) from the decrypted and/or authenticated entitlement control message is used by service demultiplexor 26 (FIG. 3) to pass encrypted service component data 64 (e.g., audio or video) to service decryptor 60. In step 142 (FIG. 7), service decryptor 60 decrypts the encrypted service component data 64 using decrypted control words as seeds 62 from decryptor 40 to provide decrypted service components 66 (FIG. 3).

Thus, before tuner 12 (FIG. 2) is tuned, an initial fast, albeit possibly unsecured, determination is made as to whether the selected service is authorized as one of the services covered by the authorized entitlement unit number stored in secure memory 38. If the selected service appears to be an authorized service, then tuner 12 is tuned to the specified frequency and the transport data stream from that specified frequency is processed. In the transport data stream corresponding to the specified frequency is an encrypted and/or authenticated entitlement control message. It is this entitlement control message that is decrypted and/or verified in secure microprocessor 30 in order to reveal, in a secure environment, the entitlement unit numbers that belong to the service. The secure microprocessor compares the list of entitlement unit numbers from the entitlement control message against the authorized entitlement unit number in memory 38 in order to determine whether the service reception is authorized in a secure microprocessor unobservable to pirates.

Since decryption is not required prior to tuning, the pre-tuning steps are performed with great dispatch. A pirate may be able to insert false entitlement unit numbers into the entitlement unit table, but not into the encrypted entitlement control message. Even though a pirate may insert a false entitlement control message into the data stream, it will not be an authenticated entitlement control message. The authentication process carried out in authenticator 34 (FIG. 3) will reveal the deception and the false entitlement control message will be disregarded. Thus, all that a pirate can accomplish is a slowing of the speed at which a user may surf through the channels.

In another embodiment, entitlement control messages are located by index. Entitlement control messages are sent in the MPEG transport stream to provide conditional access information for a given MPEG program. In this embodiment, all entitlement control messages for a given MPEG program are packed into one MPEG  
5 PID stream. This reduces the bandwidth required to transmit the entitlement control messages. Separate entitlement control messages are still associated with respective elementary streams (e.g., video or audio) by use of the stream\_index discussed below.

Entitlement control messages bearing MPEG packets are mapped to the program elements (e.g., video and each audio data stream) of an MPEG program  
10 using a conditional access descriptor (CA\_descriptor) as elementary stream (ES) information in the program level of the transport stream program map section. The CA\_descriptor identifies the entitlement control message PID that carries all of the conditional access entitlement control messages pertaining to the elementary stream associated with the extended ES information. The CA\_descriptor carried in the  
15 program map table used as extended ES information includes: a descriptor\_tag, a descriptor\_length, a CA\_system\_ID, a CA\_PID, and an ECM\_information\_descriptor.

The descriptor\_tag is preferably an 8 bit field defined by MPEG standards to be 0x09 indicating that the CA\_descriptor is for a conditional access system. The descriptor\_length is preferably an 8 bit field representing the number of bytes (or bits,  
20 etc.) of the present CA\_descriptor. The CA\_system\_ID is preferably a 16 bit field identifying the particular conditional access system to which the CA\_descriptor pertains. There may be more than one. The CA\_PID is preferably a 13 bit field carrying the PID value of the entitlement control message bearing packets for the associated elementary stream. The ECM\_information\_descriptor preferably includes  
25 one or more 24 bit fields (the number depends on descriptor\_length, above) where each 24 bit field includes: an ECM\_descriptor\_tag, an ECM\_descriptor\_length, and a stream\_index. The ECM\_descriptor\_tag is an 8 bit field that identifies a characteristic of the associated entitlement control message, for example, identifying the entitlement control message as a stream type descriptor (other descriptor types being possible).

30 The ECM\_descriptor\_length is an 8 bit field that merely identifies the remaining

length of the current ECM\_information\_descriptor (in bytes). The stream\_index is an 8 bit field that identifies the entitlement control messages in a multiple entitlement control message stream that contain information pertaining to the elementary stream associated with the CA\_descriptor.

5           Entitlement control messages for all elementary streams (e.g., video, audio, etc.) of a given program are packed into packets identified by one PID. For example, assume that an MPEG program has (1) a video stream identified by PID 100, an audio stream identified by PID 200, and an entitlement control message stream identified by PID 300. PID 300 contains entitlement control messages used by both the video and  
10           audio data streams. The entitlement control messages for each elementary stream are assigned arbitrary but unique and preferred sequential stream index values. For example, entitlement control messages for the video stream (PID 100) may be assigned a stream\_index value of 25, and entitlement control messages for the audio stream (PID 200) may be assigned a stream\_index value of 50.

15           The information contained in the transport stream program map table is used to link entitlement control messages to the correct elementary stream. The CA\_descriptor (described above) is looked up in the program map table when the program is selected. For the present example, the program map table identifies the video stream as PID 100 and the audio stream as PID 200. The program map table  
20           identified the CA\_descriptor which in turn identifies the CA\_system\_ID, the CA\_PID as 300 (in this example) and the stream\_index for the video as 25 and for audio as 50 as discussed above. Thus, home communication terminal 4 (FIG. 1) can identify the PID of the video and audio streams from program map table. Further, home communications terminal identifies one PID (using the CA\_descriptor discussed  
25           above) for all entitlement control messages associated with the present program. However, it is still possible to maintain separate entitlement control messages for each elementary stream by using the stream\_index (as discussed above) for each separate elementary stream.

          Having described preferred embodiments of a novel apparatus and method for  
30           the encapsulation of entitlement authorization in a conditional access system (which

PATENT APPLICATION  
DOCKET NO. A-6307

are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. It is therefore to be understood that changes may be made in the particular embodiments of the invention disclosed which are within the scope and spirit of the invention as  
5 defined by the appended claims.

Having thus described the invention with the details and particularity required by the patent laws, what is claimed and desired protected by Letters Patent is set forth in the appended claims.

**What is claimed is:**

1. In a terminal of a conditional access system in which a user selects a service, the selected service being associated with a frequency, the terminal having a tuner and a secure element with at least one authorized entitlement unit number stored  
5 therein, a method of determining whether the terminal is authorized to receive the selected service, the method comprising steps of:

receiving at least one encrypted entitlement control message corresponding to the service;

10 decrypting each of the at least one encrypted entitlement control message in the secure element, each decrypted entitlement control message revealing at least one first entitlement number associated with the selected service; and

determining that the terminal is authorized to receive the selected service when any first entitlement number of any decrypted entitlement control message represents any number of the at least one authorized entitlement unit number.  
15

2. The method of claim 1, further comprising initial steps of:

receiving over a permanently available link an entitlement unit table associating the selected service with at least one second entitlement number;

20 tuning the tuner of the terminal to the frequency associated with the selected service when any of said at least one second entitlement number represents any number of said at least one authorized entitlement unit number.

3. The method of claim 2, wherein the step of receiving over a permanently available data link includes receiving the entitlement unit table over an  
25 out of band data link.

4. The method of claim 2, wherein the step of receiving over a permanently available link includes receiving the entitlement unit table incorporated in a data packet that is included in a data stream associated with an initial power on  
30 frequency that is tunable by the tuner.



PATENT APPLICATION  
DOCKET NO. A-6307

5. The method of claim 2, wherein the step of receiving over a permanently available link includes receiving the entitlement unit table incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

5

6. The method of claim 1, wherein the step of decrypting the at least one encrypted entitlement control message includes recovering at least one control word associated with decryption of a video component of the selected service.

10

7. The method of claim 1, wherein the step of decrypting the at least one encrypted entitlement control message includes recovering at least one control word associated with decryption of an audio component of the selected service.

15

8. The method of claim 1, wherein the step of receiving at least one encrypted entitlement control message includes demodulating an output of the tuner to recover a data component corresponding to the selected service, the data component containing the encrypted entitlement control message.

20

9. The method of claim 1, wherein the step of decrypting said at least one encrypted entitlement control message includes recovering at least one control word from said at least one decrypted entitlement control message, each control word being a decryption key for decrypting a corresponding service component of the selected service.

25

10. The method of claim 9, further comprising steps of:  
recovering a first encrypted service component; and  
decrypting the encrypted service component using a first control word of said at least one control word.

PATENT APPLICATION  
DOCKET NO. A-6307

11. The method of claim 1, further comprising steps of:  
receiving an encrypted entitlement management message addressed to  
the terminal; and

5 decrypting the encrypted entitlement management message in the  
secure element, the decrypted entitlement management message including an update  
of at least one authorized entitlement unit number to be stored in the secure element.

12. The method of claim 11, wherein the step of receiving an encrypted  
entitlement management message includes receiving the encrypted entitlement  
10 management message over an out of band data link.

13. The method of claim 11, wherein the step of receiving an encrypted  
entitlement management message includes receiving the encrypted entitlement  
management message incorporated in a data packet that is included in a data stream  
15 associated with each frequency that is tunable by the tuner.

14. The method of claim 1, further comprising steps of:  
receiving an entitlement management message addressed to the  
terminal; and  
20 authenticating the entitlement management message in the secure  
element, the authenticated entitlement management message including an update of at  
least one authorized entitlement unit number to be stored in the secure element.

15. The method of claim 14, wherein the step of receiving an entitlement  
25 management message includes receiving the entitlement management message over  
an out of band data link.

PATENT APPLICATION  
DOCKET NO. A-6307

16. The method of claim 14, wherein the step of receiving an entitlement management message includes receiving the entitlement management message incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

5

17. In a terminal of a conditional access system in which a user selects a service, the selected service being associated with a frequency, the terminal having a tuner and a secure element with at least one authorized entitlement unit number stored therein, a method of determining whether the terminal is authorized to receive the selected service, the method comprising steps of:

10

receiving at least one entitlement control message corresponding to the service;

15

authenticating each of the at least one entitlement control message in the secure element, each authenticated entitlement control message revealing at least one first entitlement number associated with the selected service; and

determining that the terminal is authorized to receive the selected service when any first entitlement number of any authenticated entitlement control message represents any number of the at least one authorized entitlement unit number.

20

18. The method of claim 17, further comprising initial steps of:

receiving over a permanently available link an entitlement unit table associating the selected service with at least one second entitlement number;

25

tuning the tuner of the terminal to the frequency associated with the selected service when any of said at least one second entitlement number represents any number of said at least one authorized entitlement unit number.

30

19. The method of claim 18, wherein the step of receiving over a permanently available data link includes receiving the entitlement unit table over an out of band data link.

PATENT APPLICATION  
DOCKET NO. A-6307

20. The method of claim 18, wherein the step of receiving over a permanently available link includes receiving the entitlement unit table incorporated in a data packet that is included in a data stream associated with an initial power on frequency that is tunable by the tuner.

5

21. The method of claim 18, wherein the step of receiving over a permanently available link includes receiving the entitlement unit table incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

10

22. The method of claim 17, wherein the step of authenticating the at least one entitlement control message includes recovering at least one control word associated with decryption of a video component of the selected service.

15

23. The method of claim 17, wherein the step of authenticating the at least one entitlement control message includes recovering at least one control word associated with decryption of an audio component of the selected service.

20

24. The method of claim 17, wherein the step of receiving at least one entitlement control message includes demodulating an output of the tuner to recover a data component corresponding to the selected service, the data component containing the entitlement control message.

25

25. The method of claim 17, wherein the step of authenticating said at least one entitlement control message includes recovering at least one control word from said at least one entitlement control message, each control word being a decryption key for decrypting a corresponding service component of the selected service.

PATENT APPLICATION  
DOCKET NO. A-6307

26. The method of claim 25, further comprising steps of:  
recovering a first encrypted service component; and  
decrypting the encrypted service component using a first control word  
of said at least one control word.

5

27. The method of claim 17, further comprising steps of:  
receiving an encrypted entitlement management message addressed to  
the terminal; and  
decrypting the encrypted entitlement management message in the  
10 secure element, the decrypted entitlement management message including an update  
of at least one authorized entitlement unit number to be stored in the secure element.

28. The method of claim 27, wherein the step of receiving an encrypted  
entitlement management message includes receiving the encrypted entitlement  
15 management message over an out of band data link.

29. The method of claim 27, wherein the step of receiving an encrypted  
entitlement management message includes receiving the encrypted entitlement  
management message incorporated in a data packet that is included in a data stream  
20 associated with each frequency that is tunable by the tuner.

30. The method of claim 17, further comprising steps of:  
receiving an entitlement management message addressed to the  
terminal; and  
25 authenticating the entitlement management message in the secure  
element, the authenticated entitlement management message including an update of at  
least one authorized entitlement unit number to be stored in the secure element.

PATENT APPLICATION  
DOCKET NO. A-6307

31. The method of claim 30, wherein the step of receiving an entitlement management message includes receiving the entitlement management message over an out of band data link.

5 32. The method of claim 30, wherein the step of receiving an entitlement management message includes receiving the entitlement management message incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

10 33. In a terminal of a conditional access system, the terminal including a tuner and a selector for selecting a service, the selected service being identified by a corresponding service number and frequency, a conditional access apparatus comprising:

a processor having plural control modules, a first control module  
15 controlling the processor to receive at least one encrypted entitlement control message corresponding to the selected service; and

a secure element having at least one authorized entitlement unit  
number stored therein and having plural control modules, a second control module  
controlling the secure element to decrypt each of the at least one encrypted entitlement  
20 control message, each decrypted entitlement control message revealing at least one first entitlement number associated with the selected service, a third control module  
controlling the secure element to determine that the terminal is authorized to receive  
the selected service when any first entitlement number of any decrypted entitlement  
control message represents any number of the at least one authorized entitlement unit  
25 number.

34. The apparatus of claim 33, wherein:

the processor further includes a fourth control module controlling the  
processor to receive over a permanently available link an entitlement unit table  
30 associating the selected service with at least one second entitlement number; and

the processor further includes a fifth control module controlling the processor to tune the tuner of the terminal to the frequency associated with the selected service when any of said at least one second entitlement number represents any number of said at least one authorized entitlement unit number.

5

35. The apparatus of claim 34, wherein the fourth control module includes a control module to receive the entitlement unit table over an out of band data link.

36. The apparatus of claim 34, wherein the fourth control module includes  
10 a control module to receive the entitlement unit table incorporated in a data packet that is included in a data stream associated with an initial power on frequency that is tunable by the tuner.

37. The apparatus of claim 34, wherein the fourth control module includes  
15 a control module to receive the entitlement unit table incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

38. The apparatus of claim 33, wherein the second control modules  
20 includes a control module to recover at least one control word associated with decryption of a video component of the selected service.

39. The apparatus of claim 33, wherein the second control module includes  
25 a control module to recover at least one control word associated with decryption of an audio component of the selected service.

40. The apparatus of claim 33, wherein the first control module includes a control module to demodulate an output of the tuner to recover a data component corresponding to the selected service, the data component containing the encrypted  
30 entitlement control message.

41. The apparatus of claim 33, wherein the second control module includes a control module to recover at least one control word from said at least one decrypted entitlement control message, each control word being a decryption key for decrypting  
5 a corresponding service component of the selected service.

42. The apparatus of claim 41, further comprising:  
a fourth control module to control the processor to recover a first encrypted service component; and  
10 a decryptor to decrypt the encrypted service component using a first control word of said at least one control word.

43. The apparatus of claim 33, further comprising:  
a fourth control module to control the processor to receive an  
15 encrypted entitlement management message addressed to the terminal; and  
a fifth control module to control the secure element to decrypt the encrypted entitlement management message, the decrypted entitlement management message including an update of at least one authorized entitlement unit number to be stored in the secure element.

20 44. The apparatus of claim 43, wherein the fourth control module includes a control module to receive the encrypted entitlement management message over an out of band data link.

25 45. The apparatus of claim 43, wherein the fourth control module includes a control module to receive the encrypted entitlement management message incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.



PATENT APPLICATION  
DOCKET NO. A-6307

46. The apparatus of claim 33, further comprising:

a fourth control module to control the processor to receive an entitlement management message addressed to the terminal; and

a fifth control module to control the secure element to authenticate the  
5 entitlement management message, the authenticated entitlement management message including an update of at least one authorized entitlement unit number to be stored in the secure element.

47. The apparatus of claim 46, wherein the fourth control module includes

10 a control module to receive the entitlement management message over an out of band data link.

48. The apparatus of claim 46, wherein the fourth control module includes

15 a control module to receive the entitlement management message incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

49. In a terminal of a conditional access system, the terminal including a

20 tuner and a selector for selecting a service, the selected service being identified by a corresponding service number and frequency, a conditional access apparatus comprising:

a processor having plural control modules, a first control module controlling the processor to receive at least one entitlement control message corresponding to the selected service; and

25 a secure element having at least one authorized entitlement unit number stored therein and having plural control modules, a second control module controlling the secure element to authenticate each of the at least one entitlement control message, each entitlement control message revealing at least one first entitlement number associated with the selected service, a third control module  
30 controlling the secure element to determine that the terminal is authorized to receive

PATENT APPLICATION  
DOCKET NO. A-6307

the selected service when any first entitlement number of any authenticated entitlement control message represents any number of the at least one authorized entitlement unit number.

5           50.    The apparatus of claim 49, wherein:

                  the processor further includes a fourth control module controlling the processor to receive over a permanently available link an entitlement unit table associating the selected service with at least one second entitlement number; and

                  the processor further includes a fifth control module controlling the  
10   processor to tune the tuner of the terminal to the frequency associated with the selected service when any of said at least one second entitlement number represents any number of said at least one authorized entitlement unit number.

                  51.    The apparatus of claim 50, wherein the fourth control module includes  
15   a control module to receive the entitlement unit table over an out of band data link.

                  52.    The apparatus of claim 50, wherein the fourth control module includes  
a control module to receive the entitlement unit table incorporated in a data packet  
that is included in a data stream associated with an initial power on frequency that is  
20   tunable by the tuner.

                  53.    The apparatus of claim 50, wherein the fourth control module includes  
a control module to receive the entitlement unit table incorporated in a data packet  
that is included in a data stream associated with each frequency that is tunable by the  
25   tuner.

                  54.    The apparatus of claim 49, wherein the second control modules  
includes a control module to recover at least one control word associated with  
decryption of a video component of the selected service.

30

PATENT APPLICATION  
DOCKET NO. A-6307

55. The apparatus of claim 49, wherein the second control module includes a control module to recover at least one control word associated with decryption of an audio component of the selected service.

5 56. The apparatus of claim 49, wherein the first control module includes a control module to demodulate an output of the tuner to recover a data component corresponding to the selected service, the data component containing the entitlement control message.

10 57. The apparatus of claim 49, wherein the second control module includes a control module to recover at least one control word from said at least one entitlement control message, each control word being a decryption key for decrypting a corresponding service component of the selected service.

15 58. The apparatus of claim 57, further comprising:  
a fourth control module to control the processor to recover a first encrypted service component; and  
a decryptor to decrypt the encrypted service component using a first control word of said at least one control word.

20 59. The apparatus of claim 49, further comprising:  
a fourth control module to control the processor to receive an encrypted entitlement management message addressed to the terminal; and  
a fifth control module to control the secure element to decrypt the  
25 encrypted entitlement management message, the decrypted entitlement management message including an update of at least one authorized entitlement unit number to be stored in the secure element.

PATENT APPLICATION  
DOCKET NO. A-6307

60. The apparatus of claim 59, wherein the fourth control module includes a control module to receive the encrypted entitlement management message over an out of band data link.

5 61. The apparatus of claim 59, wherein the fourth control module includes a control module to receive the encrypted entitlement management message incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

10 62. The apparatus of claim 49, further comprising:  
a fourth control module to control the processor to receive an entitlement management message addressed to the terminal; and  
a fifth control module to control the secure element to authenticate the entitlement management message, the authenticated entitlement management message  
15 including an update of at least one authorized entitlement unit number to be stored in the secure element.

20 63. The apparatus of claim 62, wherein the fourth control module includes a control module to receive the entitlement management message over an out of band data link.

25 64. The apparatus of claim 62, wherein the fourth control module includes a control module to receive the entitlement management message incorporated in a data packet that is included in a data stream associated with each frequency that is tunable by the tuner.

**MECHANISM AND APPARATUS FOR ENCAPSULATION OF  
ENTITLEMENT AUTHORIZATION IN CONDITIONAL ACCESS SYSTEM**

5                                   **ABSTRACT OF THE INVENTION**

A method for determining whether the terminal is authorized to receive the selected service is practiced in a terminal of a conditional access system in which a user selects a service, the selected service being associated with a frequency, the terminal having a tuner and a secure element with at least one authorized entitlement unit number stored therein. The method includes receiving at least one encrypted entitlement control message corresponding to the service, and decrypting each of the at least one encrypted entitlement control message in the secure element, each decrypted entitlement control message revealing at least one first entitlement number associated with the selected service. The method further includes determining that the terminal is authorized to receive the selected service when any first entitlement number of any decrypted entitlement control message represents any number of the at least one authorized entitlement unit number. Alternatively, the method includes receiving at least one entitlement control message corresponding to the service, and authenticating each of the at least one entitlement control message in the secure element, each authenticated entitlement control message revealing at least one first entitlement number associated with the selected service. The method further including determining that the terminal is authorized to receive the selected service when any first entitlement number of any authenticated entitlement control message represents any number of the at least one authorized entitlement unit number.

10  
15  
20

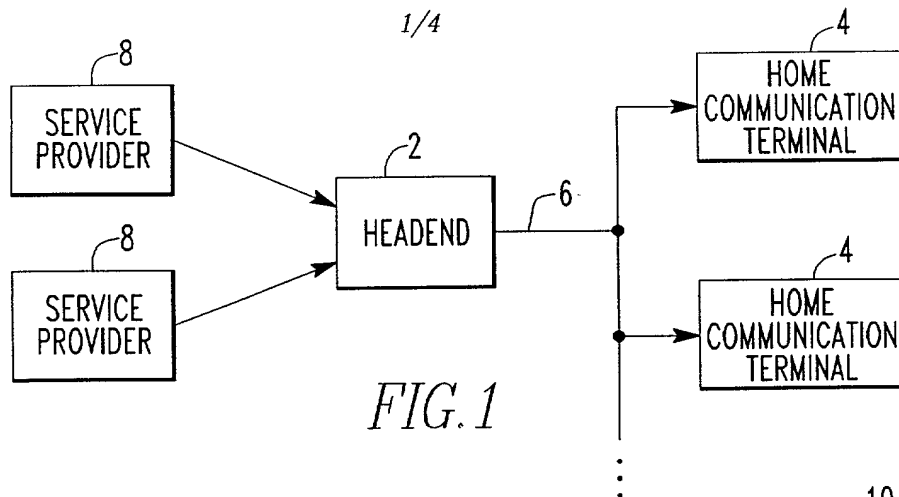


FIG. 1

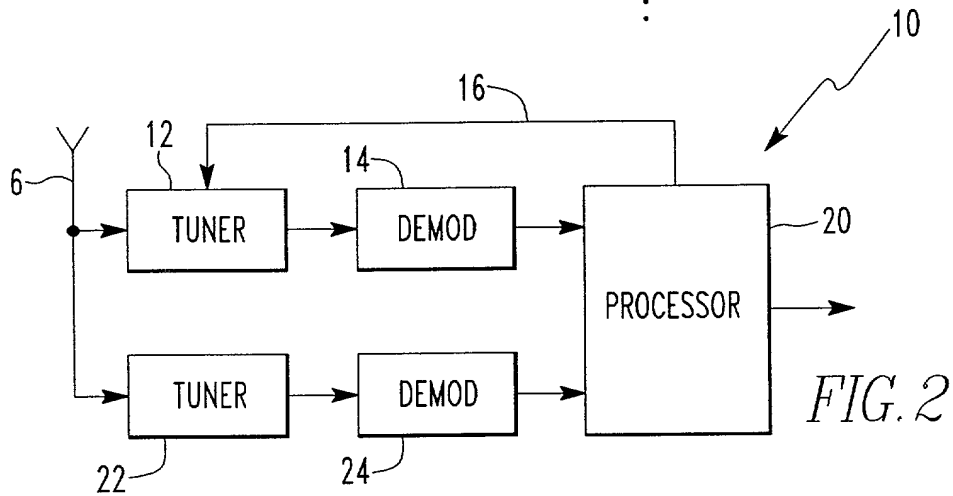


FIG. 2

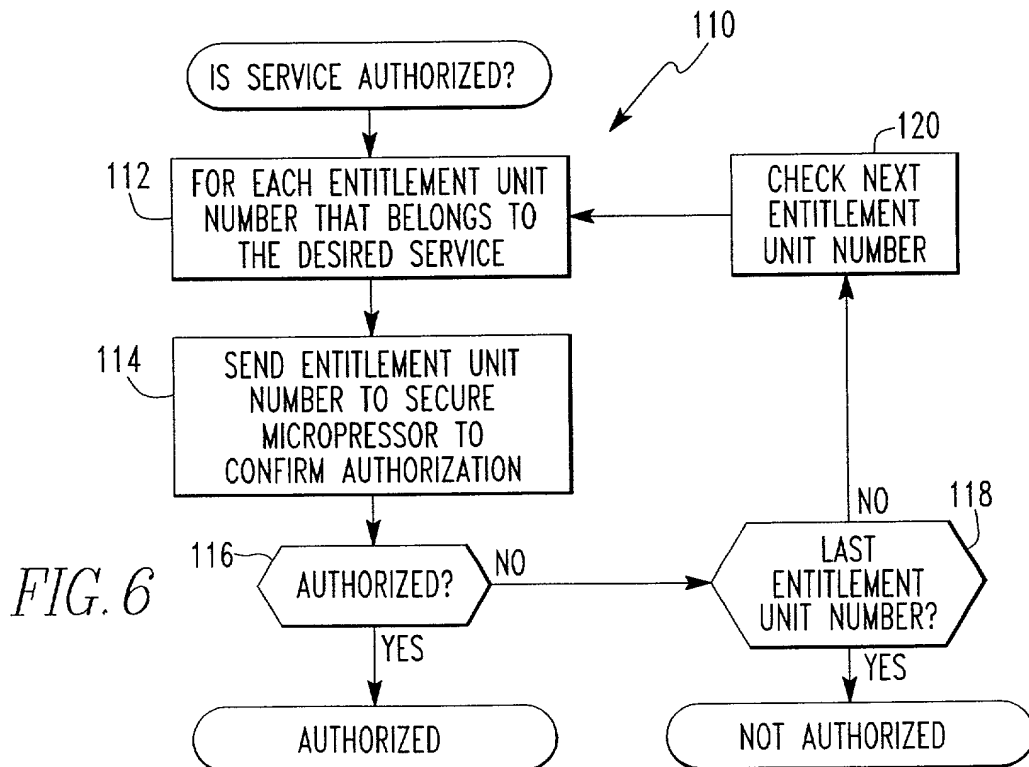


FIG. 6

FIG. 3

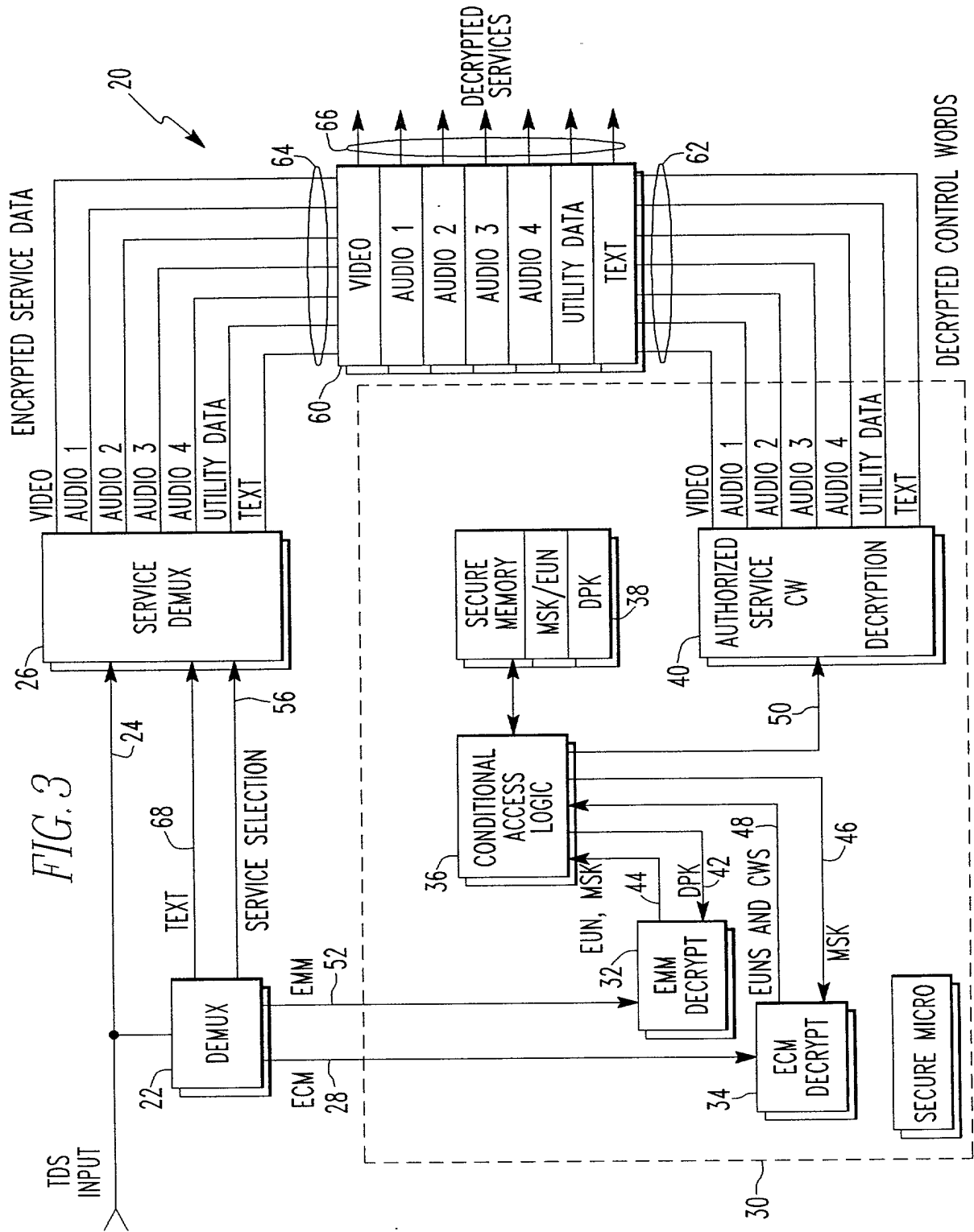
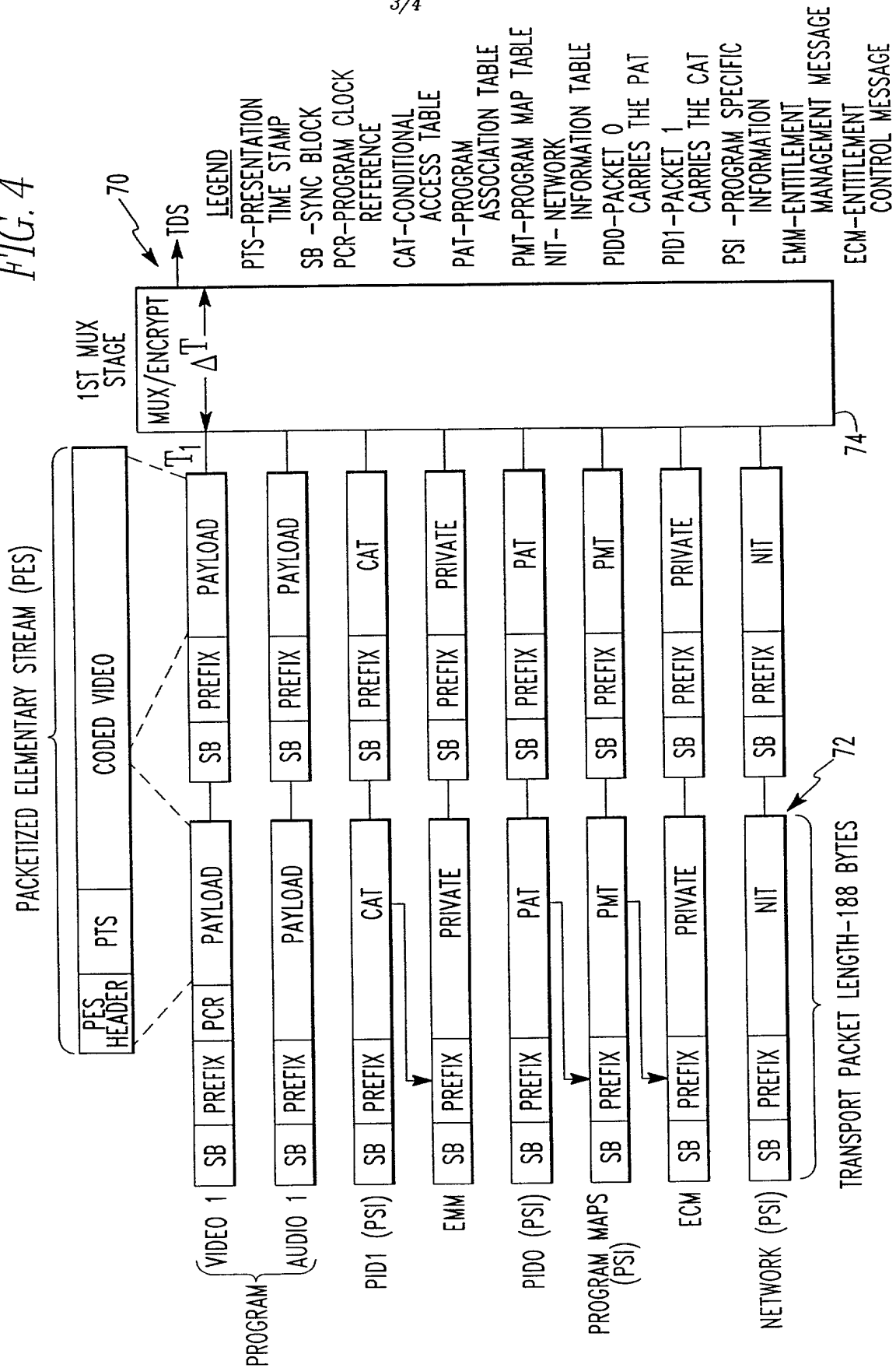


FIG. 4





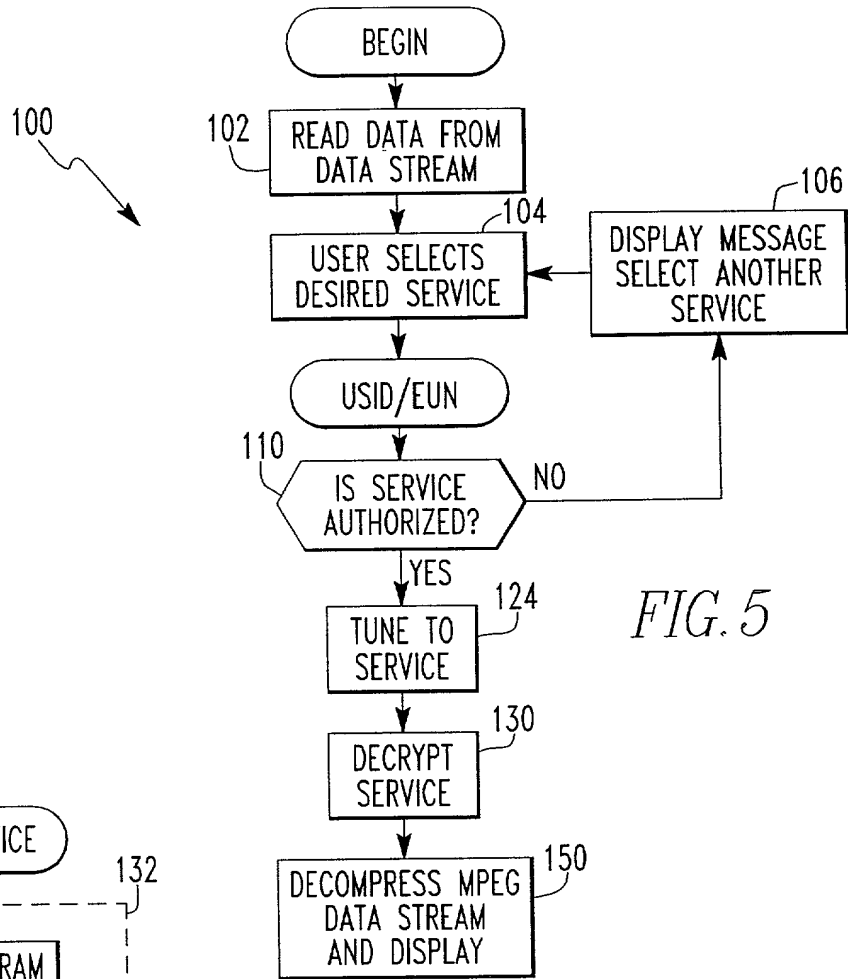


FIG. 5

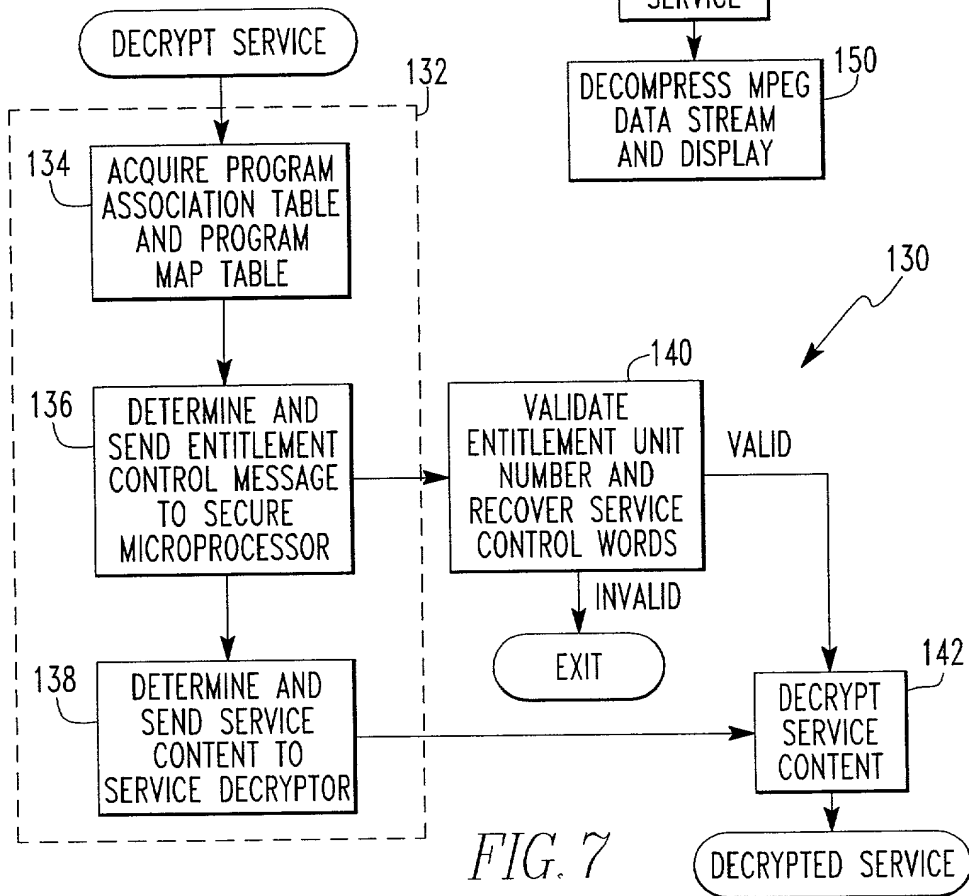


FIG. 7

**PATENT APPLICATION DECLARATION  
COMBINED WITH POWER OF ATTORNEY**

Attorney's Docket No. **A-2910**

☒ Regular (Utility)

☐ Design Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**MECHANISM AND APPARATUS FOR ENCAPSULATION OF ENTITLEMENT  
AUTHORIZATION IN CONDITIONAL ACCESS SYSTEM**

the specification of which:

☒ is attached hereto

☐ was filed on: \_\_\_\_\_

as U.S. Serial No.: \_\_\_\_\_

and was amended on \_\_\_\_\_

*(if applicable)*

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Section 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119, of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

**Prior Foreign/PCT Application(s):**

☒ no such application(s) filed.

☐ such application(s) identified as follows:

Country	Application Number	Date of Filing (day, month, year)	Priority Claimed Under 37 USC 119
			<input type="checkbox"/> Yes <input type="checkbox"/> No

I hereby claim the priority benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner

provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which is material to the examination of this application and which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

**Prior U.S. Application(s):**

- ☐ no such application(s) filed.
- ☒ such application(s) identified as follows:

Application No.	Filing Date (day, month, year)	Status (Patented, Pending, Abandoned)
60/054,578	August 1, 1997	Pending

I hereby declare that: as to any claimed subject matter of this application which is common to my earlier United States or foreign application(s), if any, which I have identified above and claimed the benefit of priority thereof, I do not believe that the same was ever known or used in the United States before my invention thereof or patented or described in any printed publication in any country before my invention thereof or more than one year prior to the first of said earlier application(s), or in public use or on sale in the United States more than one year prior to the first of said earlier application(s), and that the said common subject matter has not been patented or made the subject of an inventor's certificate before the date of the first of said earlier U.S. application(s) in any country foreign to the United States on an application, filed by me or my legal representatives or assigns more than twelve months (six months if the present application is a Design patent application) prior to the first of said earlier U.S. application(s), if any; and that, as to any claimed subject matter of this application which is not common to said earlier application(s), if any, I do not know and do not believe that the same was ever known or used in the United States before my invention thereof or patented or described in any printed publication in any country before my invention thereof or more than one year prior to the date of this application, or in public use or on sale in the United States more than one year prior to the date of this application, and that said subject matter has not been patented or made the subject of an inventor's certificate in any country foreign to the United States on an application filed by me or my legal representatives or assigns more than twelve months (six months if the present application is a Design patent application) prior to the date of this application.

I HEREBY APPOINT THE FOLLOWING AS MY ATTORNEY(S) OR AGENT(S) WITH FULL POWER OF SUBSTITUTION TO PROSECUTE THIS APPLICATION AND TRANSACT ALL BUSINESS IN THE PATENT AND TRADEMARK OFFICE CONNECTED THEREWITH:

NAME(S)	REG. NO.(S)	ASSOCIATE POWER OF ATTORNEY ATTACHED
Kenneth M. Massaroni	33,015	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Hubert J. Barnhardt III	36,739	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Kelly A. Gardner	35,147	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

Send correspondence to:

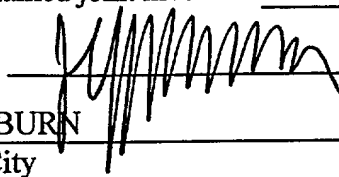
SCIENTIFIC-ATLANTA, INC.  
Intellectual Property Department  
One Technology Parkway, South  
Norcross, GA 30092-2967  
Direct Telephone Calls to: (770)903-4717

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first or sole inventor			DARRYL L. DEFREESE
Inventor's signature		<i>Darryl L. Defreese</i>	Date 7/2/98
Residence	LAWRENCEVILLE	GEORGIA	
	City	State or Foreign Country	
Citizenship	UNITED STATES		
	Country		
Post Office Address	517 COOPER'S POND		
	Street Address		
LAWRECEVILLE	GEORGIA	30044	
City	State or Country	Zip Code	

Full name of second named joint inventor JEFFREY M. SEAMAN

Inventor's signature



Date

7/02/98

Residence

LILBURN

GEORGIA

City

State or Foreign Country

Citizenship

UNITED STATES

Country

Post Office Address

3958 LEE RIDGE WAY

Street Address

LILBURN

GEORGIA

30047

City

State or Country

Zip Code

Full name of third named joint inventor <u>ANTHONY J. WASILEWSKI</u>		
Inventor's signature <u>Anthony J. Wasilewski</u>	Date <u>7/6/98</u>	
Residence <u>ALPHARETTA</u>	<u>GEORGIA</u>	
City	State or Foreign Country	
Citizenship <u>UNITED STATES</u>	Country	
Post Office Address <u>10689 WREN RIDGE ROAD</u>	Street Address	
<u>ALPHARETTA</u>	<u>GEORGIA</u>	<u>30022</u> <i>ajw</i>
City	State or Country	Zip Code